How to Cite:
Tamilselvi, R., & Indumathi, A. (2022). Adaptive secured position based routing protocol for efficient data transmission in Vehicular Adhoc network. *International Journal of Health Sciences*, *6*(S6), 3025–3032. https://doi.org/10.53730/ijhs.v6nS6.10266

Adaptive secured position based routing protocol for efficient data transmission in Vehicular Adhoc network

Dr. R. Tamilselvi
Head & Assistant Professor, Department of Computer Applications, Erode Arts and Science College, Erode-9
Email: rtamilu.sundar@gmail.com

Dr. A. Indumathi
Associate Professor, Department of Computer Application, Kongunadu Arts and Science College, Coimbatore -29
Email: Indumathia_ca@kongunaducollege.ac.in

***Abstract*---**Variable number of cars equipped with radio devices allow the driver to exchange messages seamlessly across the network, no matter where they are in relation to each other. Inter-vehicle video transmission is an important feature of the VANET. Foreseeing the development of commercial service, video streaming appears to be a practical answer to a number of expected services. For data transmission in vehicular ad hoc networks, this study examines non-delay-tolerant and delay-tolerant network protocols, respectively.Different performance metric criteria like Packet Loss ratio, Number of Packet delivered, Route Length are evaluated.

***Keywords*---**VANET, Non DTN, DTN

Introduction

Another development that blends the potential of modern remote systems into automobiles is the Vehicular Ad-hoc Network (VANET). VANET plans to provide:

- Persistent availability for a variety of clients when they are out and about, allowing them to communicate with those clients through their own home or office systems, and
- Productive remote association between vehicles without access to any established basis, which gives the ITS more power. In other words, VANET is another name for IVC (IVC). A good example of a VANET device is a vehicle-mounted equipment that serves as a hub for communications being

sent and received via distant systems. These devices provide the most up-to-date information about accidents, flooding, precipitation, crowded roads and other aggravations to drivers and travelers. When drivers get access to this information early on, they may make the best decisions possible and avoid accidents.

A VANET is comparable to the activity innovation of a Mobile Ad hoc Network (MANET) in terms of self-association, self-administration, low transfer speed, and shared radio transmission circumstances. A fundamental operational challenge for virtual ad hoc networks (VANET) arises due to the fast and temporary movement of mobile hubs (vehicles). Due to this reality, it is clear that enhancing the MANET architecture is necessary in order to successfully compel the swift movement of VANET hubs. This subject has brought together a variety of study challenges with the concept for an adequate guiding convention.

VANET Architectures

Both VANETs and MANETs have standards that are similar in that they both rely on a constant foundation for communication and information broadcasting. VANET is concerned about the ever-shifting landscape of road transportation. Figures depicting the pure cellular/WLAN, pure ad hoc, and crossbreed VANET designs are shown.

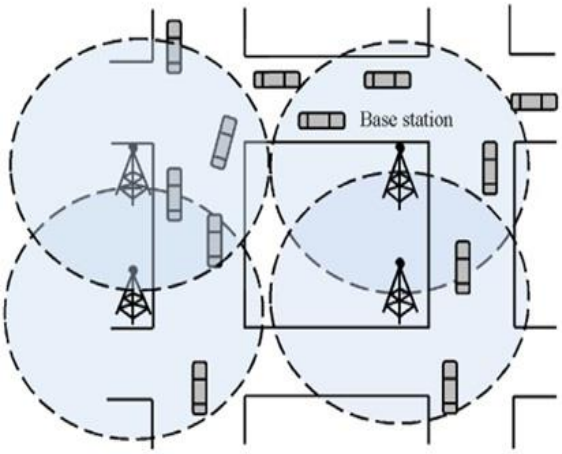


Figure 1.2. Pure Cellular

Changeless cell gateways and Wi-Fi access points and base stations at traffic intersections can be used to access the Internet, collect traffic data, or steer VANETs in a cellular system(Figure 1.2). A cellular or WLAN-based network design is required by these limitations. VANET engineering uses a range of wireless protocols, including IEEE 802.11, IEEE 802.16e, and 3G cellular frameworks, for what is known as Vehicle-to-Infrastructure (V2I) communication (Akyildiz et al., 2010; Sharef et al., 2012).

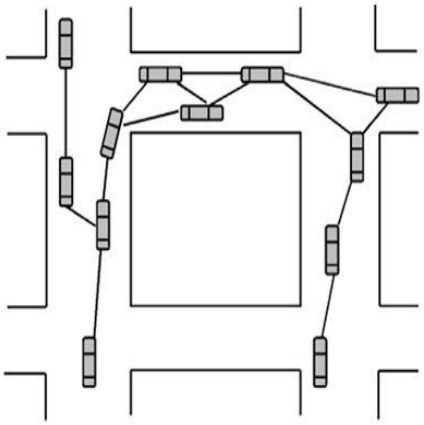


Figure 1.3. Pure Ad Hoc (V2V)

VANET's Pure Ad Hoc architecture, also known as Vehicle-to-Vehicle (V2V) correspondence, is shown in Figure 1.3. As cell towers and remote routes are constrained by a lack of funding, the hubs in this design may be forced to come closer together to form a single structure. As a result of the data collected by sensors installed in automobiles, emergency services and law enforcement agencies would be able to better track down and apprehend offenders (Namboodiri et al., 2004). In the entire ad hoc gathering where the hubs execute V2V communication, the network setup is framework-less. Figure 1.4 shows the hybrid architecture of VANET (V2I and V2V). In the hybrid design, communication between distant systems management devices may be facilitated by using roadside communication units such cellular towers, roadways, and automobiles. In a wide range of applications, foundation communication units have been used to access dynamic and well-off data beyond their system structure and communicate this data through a common ad hoc, framework less communication. More extravagant substance and unrivaled adaptability in substance exchange are provided by the hybrid architecture of cell/WLAN and ad hoc.

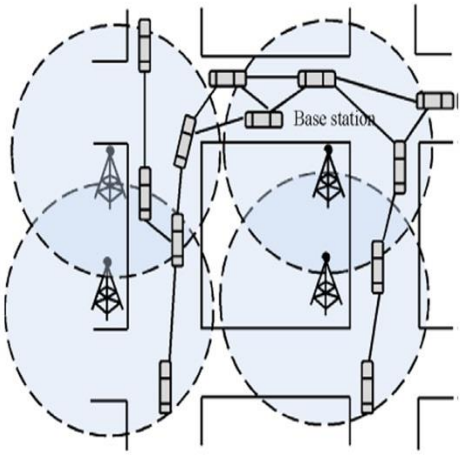


Figure 1.4. Hybrid (V2I &V2V)

Routing protocols in VANET

Routing is the process of deciding where traffic should go, whether it's within a network or between or across networks. A router is a specialized piece of hardware that is responsible for routing traffic. Routing protocols are used to communicate between cars in VANET technology.

Position Based Routing Protocol

The GPS system, which is based on location services, was used to acquire node information for position-based routing protocols. There is no need for a routing table or link state information when using position-based protocols. For better routing in automotive networks, the Position Based Routing Protocol uses vehicle position data. The nodes' geographic information is utilized in these kinds of protocols. Once the final destination has been located, a path may be devised to transport the data there. In a greedy routing, the data is sent to the node nearest to the destination. The fundamental advantage of these protocols is that the global path from the point of origin to the point of destination does not need to be established. Position-based procedures have been used in this work. One of them is a DTN. The DTSG (Dynamic Time-Stable Geocast Routing) position-based protocol and the DTN GeOpps (Geographical opportunistic routing) position-based protocol are both used in the Vanet for data transfer. Pre-stable and stable periods of DTSG are ineffective in protecting against intruders.

When problems with VANET communication arise, the DTN protocol can be used to communicate. The navigation system uses the GeOpps protocols to identify the vehicle that is most likely to arrive at the packet's closest destination. GeOpps predicts the arrival time of a packet based on the distance between the destination and the closest point on the vehicle's path. If a node has a minimum arrival time while forwarding packets, the packet will be sent to that node. In order to improve security features Security algorithms are taken into account. Data authentication, Data integrity is taken as important consideration in Security algorithms. It is one of the most secure symmetrical encryption algorithms, the Advanced Encryption Standard (AES). This research mainly focuses to reduce the packet loss ratio and to enhance the quality of data transmission. A Multipath is constructed using routing mechanishm. Here; use dimproved symmetric encryption algorithm with time slot allocation.

Proposed Method of Secured Broadcasting in VANET

Data is encrypted and decrypted using the same secret key in AES, which is known as a symmetric-key algorithm (SKA). AES utilizes a 128-bit block cipher to encrypt data. 256-bit keys need 14 rounds of encryption, whereas 128-bit keys require 10 rounds of processing. ˆ Every round is the same, with the exception of the last one in each scenario. AES utilizes a 4 4 array of bytes in column-major order for its operations.AES algorithm follows feistel structure and using block cipher design principle technique. In Feistel Structure plain text will be divided into two equal parts. Based on security level number of rounds will be generated.Subkey is generated for each round.

Encryption

For the sake of encryption, each round is divided into four segments. The key can be added, rows can be shifted, columns can be mixed, and bytes can be replaced. Following the previous three phases, the final step is to XOR the output with four words from the key schedule.

Decryption

There are four stages in each cycle of decryption: Avi Kak's Round 12 Computer and Network Security Lecture Examples of inverted shifts and inverted replacements include the 8 key, inverse shift rows, inverse bytes, and inverse mix columns. The output of phases one and two are XORed with four words from the key schedule in the third step. This is a byte-for-byte replacement utilizing a rule that is constant across all rounds of encryption. The byte-by-byte

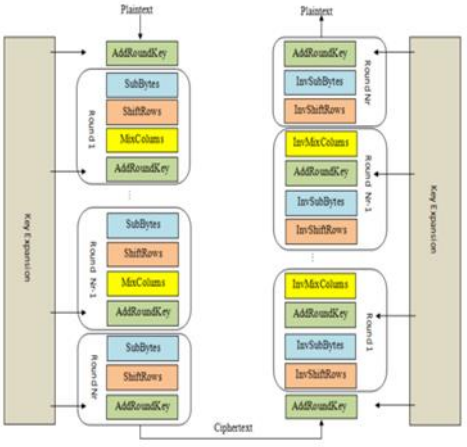


Figure 3.1. Overall structure of encryption and decryption in Advanced Encryption

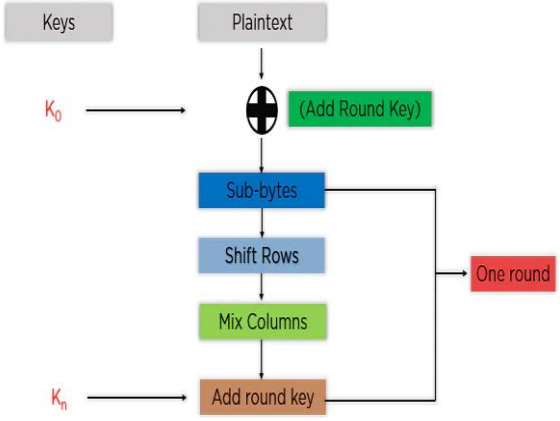
The decryption chain's standard replacement rule varies, although it remains the same throughout all rounds.

AES Algorithm with time slot

- KeyzExpansion – The cipher key is used to generate round keys using the AES key schedule. Another 128-bit key block is needed to implement AES.
- Initial round key addition:
  AddRoundKey – Bitwise xor is used to combine one byte of the round key and one byte of each byte of the state.
- 9, 11 or 13 rounds:
  - SubBytes – lookup tables are used to replace one byte with another according to a non-linear substitution step.
  - ShiftRows – The state's last three rows are moved a certain amount of times during a transposition phase.

- MixColumns – Each state column's four bytes are combined using a linear mixing technique.
- AddRoundKey

- Final round (making 10, 12 or 14 rounds in total):
  - SubBytes
  - ShiftRows
  - AddRoundKey
- timeslot allocation
  - actualbyte←UpdateResource
  - min Pbyte←min
  - TimeSlotbyte[t] ←min
  - affectedR←affectedRequest
  - end
  -



Simulation Settings, Results and Discussions

Route length, the number of packets delivered, and the packet loss ratio are the performance measures used in this study to evaluate the proposed work's efficiency.

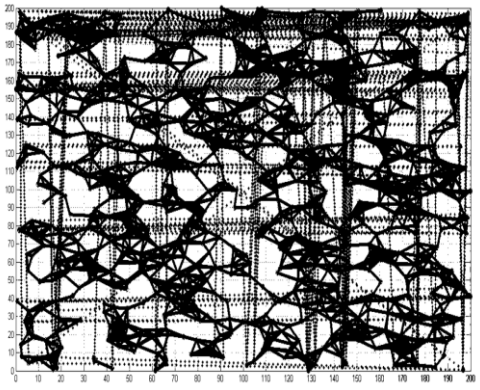


Figure 4.1 Network setup

Based on the measured performance measurements, the AMGR protocol and the suggested non-delay-tolerant network protocols. The total number of vehicular nodes in the network is 1000. Figure.6.1 shows the network set-up in action. The quality of data transmission improves as the route length increases, according to the network structure. To determine how effective the protocol is, one counts the total number of packets that have been successfully delivered. This is a measurement known as throughput, which is also referred to as the number of packets delivered.

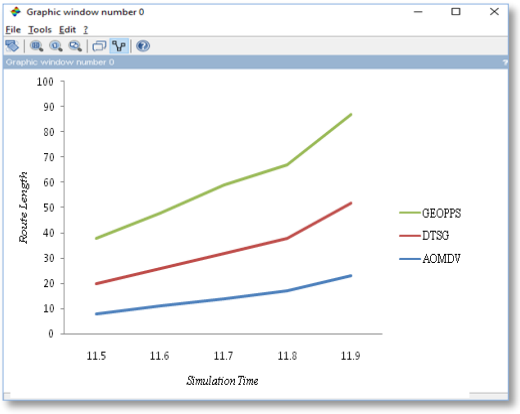


Figure 4.2 shows Number of Routelength extended

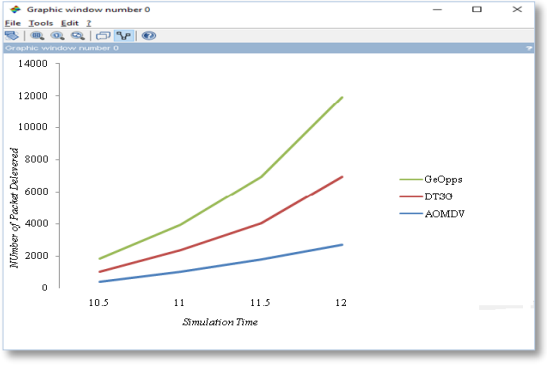


Figure 4.3 shows Number of Packets Delivered

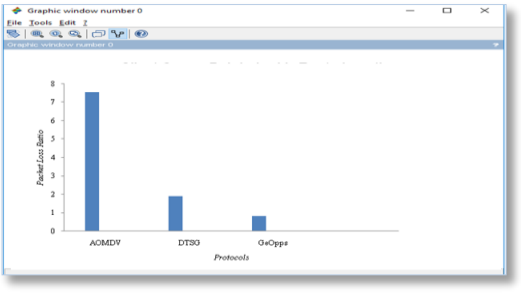


Figure 4.4 shows Packet Loss Ratio

Conclusion

This research work aimed to develop routing protocols that are capable enough to perform efficient DATA transmission in VANETs. Here , considered 2 parameters for effective data transmission are Security and timeslot. Based on experimental results it was proven that Delay-tolerant outperforms the rest of the protocols in terms of extended route length, increased packet delivery, and less packet loss ratio.

References

1. Akyildiz IF, Gutierrez-Estevez DM, Reyes EC. “The evolution to 4G cellular systems:LTE-Advanced”. Physical Communication, vol. 3, no.4, pp. 217-244, 2010.
2. Namboodiri V, Agarwal, M, Gao, L. “A study on the feasibility of mobile gateways for vehicular ad-hoc networks”,in: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks; 2004, pp. 66–75.
3. Lee U, Zhou B, Gerla M, Magistretti E, Bellavista P, Corradi A. “Mobeyes: smart mobs for urban monitoring with a vehicular sensor network”. IEEE Wireless Communications, vol. 13, no.5, pp. 52-57, 2006.
4. Hartenstein H, Laberteaux KP. A “tutorial survey on vehicular ad hoc networks”, IEEE Communications Magazine, vol. 46, no. 6, pp. 164-171, 2008.
5. Dr.V.Kathiresan R.Tamilselvi,” A Review On Routing Protocols In Vanet”International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vOl6 , Issue . 9 , pp 1355-1363,2017
6. Korkmaz G, Ekici E, Özgüner F, Özgüner Ü. “Urban multi-hop broadcast protocol for inter-vehicle communication systems”. In: Proceedings of the 1st ACM international workshop on vehicular ad hoc networks; 2004. pp. 76–85.
7. Zeadally S, Hunt R, Chen YS, Irwin A, Hassan A. “Vehicular ad hoc networks (VANETs): status, results, and challenges”. Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.
8. Arnawa, I.K., Sapanca, P.L.Y., Martini, L.K.B., Udayana, I.G.B., Suryasa, W. (2019). Food security program towards community food consumption. *Journal of Advanced Research in Dynamical and Control Systems, 11*(2), 1198-1210.
9. Gede Budasi, I. & Wayan Suryasa, I. (2021). The cultural view of North Bali community towards Ngidih marriage reflected from its lexicons. *Journal of Language and Linguistic Studies*, *17*(3), 1484–1497
10. Gandamayu, I. B. M., Antari, N. W. S., & Strisanti, I. A. S. (2022). The level of community compliance in implementing health protocols to prevent the spread of COVID-19. International Journal of Health & Medical Sciences, 5(2), 177-182. https://doi.org/10.21744/ijhms.v5n2.1897